AO 91 (Rev. 08/09) Criminal Complaint

FILED
JAN 24 2013
CLERK, U.S. DISTRICT COURT
RICHMOND, VA

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

United States of America
v.
DAVID EDWARD SLEEZER

Case No. 3:13MJ033

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 9/29/2012 to 1/23/2013 in the county of Hanover in the Eastern District of Virginia, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)	Distribution and Receipt of Child Pornography

This criminal complaint is based on these facts:

Attached affidavit, which is fully incorporated by reference herein.

☑ Continued on the attached sheet.

Complainant's signature

Linsey Bosnich FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 01/24/2013

/S/
David J. Novak
United States Magistrate Judge
Judge's signature

City and state: Richmond, Virginia

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Linsey F. Bosnich, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a criminal complaint and arrest warrant under Rules 3 and 4 of the Federal Rules of Criminal Procedure for DAVID SLEEZER, for distribution and receipt of child pornography, in violation of Title 18, United States Code, Section 2252A(a)(2).

2. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and have been since March 2010. I am thus an officer of the United States who is empowered by law to conduct investigations of, and make arrests for, offenses enumerated in Title 18, United States Code, Section 2252 and Title 18, United States Code, Section 2252A.

3. I am currently assigned to the investigation of cases involving crimes against children. These investigations have included the use of surveillance techniques, undercover activities, the interviewing of subjects and witnesses, and the planning and execution of search, arrest, and seizure warrants. I have participated in investigations involving sexual assaults, pedophiles, preferential child molesters, persons who collect and distribute child pornography, and the importation and distribution of materials relating to the sexual exploitation of children. I have received training from the FBI in the areas of sexual assaults and

child exploitation, and I have reviewed images and videos of child pornography in a wide variety of media forms, including computer media. I have also discussed and reviewed these materials with other law enforcement officers.

4. The following affidavit is based on my personal experience, my conversations with other law enforcement officers, as well as my examination of documents and evidence related to this case, and it is true and correct to the best of my knowledge.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested complaint and arrest warrant, and does not set forth all facts known either to me or other law enforcement agents about this matter.

RELEVANT STATUTORY PROVISIONS

6. **Distribution or Receipt of Child Pornography**: 18 U.S.C. § 2252A(a)(2) provides that it is a crime to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

7. **Child pornography** means any visual depiction, in any format, of sexually explicit conduct where: (A) the production involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital or computer-generated image that is substantially indistinguishable from that of a minor engaged in sexually explicit conduct; or (C) such visual depiction has been

created, adapted, or modified to appear that an identifiable minor is engaged in sexual explicit conduct. *See* 18 U.S.C. § 2256(8).

8. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a visual image, and data which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

9. **Minor** means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

10. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

DEFINITIONS

11. The **Internet** is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

12. **Internet Protocol address (or simply "IP address")** is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

13. **Storage medium** is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

14. **Log Files** are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

15. **"P2P"** is shorthand for peer-to-peer. P2P file sharing is a method of communication available to Internet users through the use of special software. The software is designed to allow users to trade digital files through a network that is formed by linking computers together. A significant distinction between P2P networks and traditional computer networks is that P2P machines generally communicate directly with each other, rather than through a relatively low number of centrally-based servers. Because of the decentralized nature of P2P networks, they are commonly used by collectors and traders of child pornography.

16. **Media Access Control ("MAC")** address is a unique identifier assigned to a network interface, or network card, for identification and communications on the network. MAC addresses are most often assigned by the manufacturer of the network card, and generally do not change.

PROBABLE CAUSE

16. On September 29, 2012, and October 9, 2012, FBI Special Agent Lisa Hill connected to the Internet in an online undercover capacity. Utilizing the ARES P2P network, she connected directly to IP address 24.131.9.37 using a law enforcement version of the ARES P2P file sharing program. While connected to this IP address, she obtained a list of files the user of this IP address was sharing.

17. SA Hill viewed the list of files available from the aforementioned IP address, and based on her training and experience determined the filenames were consistent with child pornography. SA Hill subsequently initiated several "single-

source" downloads.[1] SA Hill downloaded two video files and one still image of suspected child pornography. The following are descriptions of the downloaded files:

a. File Title: **cbaby-toddler girl katy [daddy cums again part 2] (4).mpg**

DESCRIPTION: This is a video file approximately twenty four seconds in length. This video depicts what appears to be a female toddler using her hands to spread the lips of her vagina open while an erect adult penis urinates or ejaculates onto her vagina and anus.

b. File Title: **(pthc) kgirl – anal.avi**

DESCRIPTION: This is a video file that is approximately three minutes and four seconds in length. The video depicts what appears to be a female child of approximately four to six years of age performing oral sex on an adult male. Thereafter, she lies on her stomach and spreads her buttocks apart with her hands as the adult male penetrates her anus with his erect penis.

c. File Title: **mixed pics pthc ptsc young ones-37(2)(2).jpg**

DESCRIPTION: This is a still image file. This image depicts what appears to be an approximately six to nine-year-old female child restrained by ropes and being lifted off the ground by her vagina.

---

[1] Some P2P applications permit simultaneous downloading of different parts of the same file from multiple computers (connected to the Internet via different IP addresses) to accelerate the downloading process. The law enforcement version of the P2P application used in this investigation was configured to force downloading from a "single source," *i.e.*, a single IP address, to ensure that the entirety of the suspect files would be downloaded from only one computer, *i.e.*, the target IP address.

18. During the downloading of the above files, other incoming data were captured. SA Hill confirmed all three above-described suspected child pornography files were downloaded from the same IP address.

19. According to an open source Internet research tool, IP address 24.131.9.37 is owned by Comcast Cable Communications. Comcast Cable Communications records indicated that during the time of the above-referenced child pornography downloads the IP address was assigned to an account subscribed in the name of Cindi Coleman, with service provided to 8264 J David Lane, Mechanicsville, VA, 23111.

20. A search of CLEAR, a subscriber-only public records database, revealed another resident at 8264 J David Lane, named James Thomas Hall. CLEAR listed the owners of the residence as James Hall and Cindi C, husband and wife.

21. On November 16, 2012, agents from the FBI executed a Federal search warrant at the residence of James and Cindi Hall located at 8264 J David Lane, Mechanicsville, VA, 23111.

22. On November 16, 2012, pursuant to the Federal search warrant, Cindi and James Hall were interviewed. Both James and Cindi Hall informed the Investigators they had never downloaded child pornography. An on scene forensic preview of the Hall's digital media did not reveal any evidence of child pornography on Hall's computers. Additionally, at the time of the search warrant the Hall's D-

Link Systems wireless internet router was searched. The MAC and IP addresses connected to the Hall's D-Link Systems router were captured.

23. A full forensic examination of digital items seized from the Hall residence pursuant to the federal search warrant did not reveal child pornography. It was determined the Hall's did not download child pornography.

24. After the federal search warrant was executed and digital items seized from the Hall residence, federal investigators obtained additional evidence that child pornography was continuing to be downloaded via the ARES P2P network to IP addresses associated with the Hall's residence.

25. On December 1, 2012, FBI Task Force Officer (TFO) Kevin Hiner connected to the Internet in an online undercover capacity. Utilizing the ARES P2P network, he connected directly to IP address 76.104.122.122 using a law enforcement version of the ARES P2P file sharing program. While connected to this IP address, he obtained a list of the files the user of this IP address was sharing.

26. TFO Hiner subsequently initiated a "single-source" download. TFO Hiner downloaded one video file of suspected child pornography. The following is a description of the downloaded file:

a. File Title: **al.avi**

DESCRIPTION: This is a video file approximately two minutes and forty four seconds in length. This video depicts what appears to be a female toddler being vaginally penetrated by an erect adult penis. In this video the male ejaculates on the toddler's vaginal area.

27. Comcast records revealed the IP address 76.104.122.122 was assigned to Cindi Coleman, 8264 J David Lane from November 30, 2012 to December 28, 2012.

28. On December 17, 2012, James Hall was interviewed at his residence by your Affiant. Hall consented to a search of his D-Link Systems router. Hall provided FBI personnel with all of the electronic devices utilized by him and his wife, and FBI personnel noted the MAC addresses for each device.

29. Examination of the logs and configuration of the wireless router at the Hall's residence indicated a network device with a host name of "davids" and a Media Access Control (MAC) address of 00:08:54:8f:b0:fb (hereafter "the TARGET MAC") connected to the Hall's wireless router on or about December 16, 2012. FBI personnel were unable to identify any electronic devices in the Hall's residence with the hostname "davids." Because the device with the TARGET MAC and hostname "davids" was connected to the Hall's wireless router, all subsequent network communication between the device with the TARGET MAC and hostname "davids" would appear to originate from the Hall's assigned IP address of 76.104.122.122.

30. On December 18, 2012, James Hall consented to the installation of monitoring equipment on the D-Link Systems wireless router located at his residence at 8264 J David Lane, Mechanicsville.

31. On December 20, 2012, your Affiant and FBI personnel installed the consensual monitoring equipment on James and Cindi Hall's D-Link Systems wireless router at their residence located at 8264 J David Lane, Mechanicsville, VA.

32. Subsequent to the installation of the consensual monitor, the TARGET MAC viewed webpages from the social networking website Netlog located at en.netlog.com. On or about December 29, 2012, the TARGET MAC viewed a webpage titled "Thread with Tina on Netlog." The webpage showed "mallsgrl" as the user signed into the Netlog website and contained messages between usernames "mallsgrl" and "tinasfun." In one of the messages, user "mallsgrl" provided the following two email addresses: mallsgrl@aol.com and mallsgrl@yahoo.com.

33. On January 15, 2012, AOL, Inc., (hereafter "AOL") provided the following account information for mallsgrl@aol.com:

> Address Information: David Sleezer, 122 Downing Road, Dewitt, NY, 13214
> Account Status: Active
> Member Since: 97-12-28
> Billing Method: Credit Card
> CC Name: David Sleezer
> Screen Names: DSle672903; Dewitt132; Mhooper99; Mallsgrl; Mallsgy.

34. AOL also provided the IP address login history information for mallsgrl@aol.com. On approximately 78 occasions "mallsgrl" logged into the aforementioned email account utilizing the IP address 24.131.9.37 during the time period September 14, 2012, to November 15, 2012. Comcast records reveal IP

address 24.131.9.37 was assigned to Cindi Coleman, 8264 J David Lane, Mechanicsville, VA, from June 29, 2012, to November 19, 2012.

35. Comcast further revealed the IP address 76.104.122.122 was assigned to Cindi Coleman, 8264 J David Lane from November 30, 2012, to December 28, 2012. On approximately 32 occasions between November 30, 2012, and December 28, 2012, "mallsgrl" logged into mallsgrl@aol.com utilizing IP 76.104.122.122, which Comcast had assigned to Cindi Coleman.

36. The computer trespasser on the Hall's wireless internet router also utilized IP address 76.104.122.122 (assigned to Cindi Coleman) to download child pornography on December 1, 2012, as previously discussed in paragraphs 22-24.

37. Upon the identification of the computer trespasser utilizing a MAC address with the hostname, "davids" and the subpoena return information from AOL in the name of David Sleezer, FBI SA Michael Schuler searched the publically available website www.hanovercountygis.org for the names of neighbors in the vicinity of 8264 J David Lane. This website listed a David E. Sleezer as the owner of 8275 J David Lane ("the PREMISES"), which is located near the Hall's residence at 8262 J David Lane. A further search of residences located in the vicinity of 8264 J David Lane revealed the PREMISES to be the only property having an owner with the first name "David" and the last initial "S."

38. Various records and databases were searched for information regarding the PREMISES:

a. A search of CLEAR, a subscriber-only public records database, listed Sleezer as the sole owner of the property and a single man.

b. Virginia Department of Motor Vehicle (DMV) records indicate David Edward Sleezer currently is licensed and assigned a Virginia license number, registered to the "PREMISES" and born in 1967, Security Number XXX-XX-8318.

39. On January 14, 2012, your Affiant and FBI personnel located the TARGET MAC via technical means and determined the MAC was located at or near 8275 J David Lane, the residence of DAVID SLEEZER.

RESULTS OF JANUARY 23, 2013 SEARCH WARRANT

40. On January 22, 2013, United States Magistrate Judge David J Novak issued search warrant, Case No. 3:13-MS-11, for the residence located at 8275 J David Lane, Mechanicsville, 23111. On January 23, 2013, the search warrant was executed by FBI agents, employees and task force officers at approximately 7:30PM.

41. Upon execution of the search warrant, the owner and sole resident of 8275 J David Lane, DAVID SLEEZER, was interviewed by your Affiant and FBI SA Michael French. SLEEZER confirmed he is the owner and sole resident of 8275 J David Lane. SLEEZER said he does not pay for internet service at his residence. SLEEZER owns a computer and purchased the computer a number of years ago while he was still residing in New York. SLEEZER said he is the only individual using the computer and he also has a USB thumb drive next to his computer on which he stores files. SLEEZER said he also burns CD's on his computer. SLEEZER said he does not download or view child pornography and has never done

so in the past. SLEEZER denied using the ARES peer-to-peer program or visiting the social networking sit Netlog (see paragraph 32 above). SLEEZER stated that he had not engaged in any online chatting since he moved to Virginia from New York a number of years ago.

42. At the time the search warrant was executed, a computer was found at the residence. The computer was on and actively operating in a non-sleep mode at the time agents entered the residence. FBI employees trained in computer forensics conducted an on-scene triage and preview using certified forensic tools designed to cause only minimal changes to the target computer's operating system and associated metadata. During that on-scene preview they examined part of the computer's operating system known as the Windows Registry[2], which listed the computer name as "Davids" and the registered owner "David Sleezer" as the only user on the system. The Registry revealed the computer was last turned on at approximately 7:17PM on January 23, 2013. A further examination of the computer's operating system revealed that at the time of the search SLEEZER's computer was connected to the Internet network subscribed to by SLEEZER's neighbors James and Cindi Hall.

43. Significantly, examination of SLEEZER's computer also revealed that it had a network card with a Media Access Control (MAC) address of

---

[2] The Windows Registry is a hierarchical database that stores information about configuration settings and options on Microsoft Windows operating systems.

00:08:54:8f:b0:fb, which is the same as that which had previously accessed the Halls' unsecured wireless router on or about December 16, 2012.

44. Contrary to SLEEZER's denial, investigators found that the ARES P2P program was running on the computer and 51 files where available in the shared folder. The file title names were indicative of child pornography. A thumb drive containing approximately 4 GB of child pornography was also recovered, along with approximately 7 CDs containing child pornography. The following are descriptions of three files found in the ARES shared folder on SLEEZER's computer:

a. File Title: **(pthc) toddler girl - !!!new dori neocompilation**

DESCRIPTION: This is a video file approximately four minutes and five seconds in length. This video depicts what appear to be two prepubescent girls approximately three to five years of age. The girls' genitalia are displayed and tweezers are inserted into the vagina of one of the girls. An adult hand rubs the girl's vagina and a stick is inserted into the girl's rectum. A hypodermic needle is inserted into the girl's vagina.

b. File Title: **(pthc) tara 9yr – masturbates vibrator and double fingers – august 22nd, 2007**

DESCRIPTION: This is a video file approximately five minutes and forty nine seconds in length. The video depicts what appears to be a prepubescent female naked on a bed and wearing a mask on her face. The girl uses a vibrator on her vagina and masturbates herself.

c. File Title: **(new) 6yr_taste (w-sound)**

DESCRIPTION: This is a video file approximately one minute and twenty three seconds in length. This video depicts what appears to be a prepubescent female bent over displaying her vagina and buttocks. The female touches an erect adult penis and puts her hand on the penis and puts the penis in her mouth.

CONCLUSION

45. I submit that this affidavit supports probable cause for ~~a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.~~ a complaint and arrest warrant for DAVID SLEEZER for distribution and receipt of child pornography.

Respectfully submitted,

Linsey Bosnich

Linsey F. Bosnich
Special Agent
FBI

Subscribed and sworn to before me
on January 24, 2013:

/S/
David J. Novak
United States Magistrate Judge

UNITED STATES MAGISTRATE JUDGE